



THE PROSECUTOR LAW REVIEW

DITERBITKAN OLEH PUSAT STRATEGI KEBIJAKAN
PENEGAKAN HUKUM, KEJAKSAAN AGUNG

P - ISSN : 2987 - 7342 E - ISSN : 2987 - 8314

AVAILABLE ONLINE
<https://prolev.kejaksaan.go.id/>



Prosecuting the Digital Frontier: Law Enforcement in Crypto Seizures

Penuntutan Aset Digital: Penyitaan Aset Kripto

Rita Komalasar¹, Cecep Mustafa²

¹ Yarsi University, Indonesia

² Stirling University, Inggris

Article Info

Corresponding Author:

Penulis Korespondensi

✉ rita.komalasari161@gmail.com

History:

Submitted: 15-01-2025

Revised: 24-08-2026

Accepted: 26-08-206

Keyword:

Blockchain Analytics;
Cryptocurrency Seizure, Digital
Asset, Prosecuting.

Kata Kunci:

Analisis Blockchain; Penyitaan
Cryptocurrency; Aset Digital;
Penuntutan.



Copyright © 2026 by
The Prosecutor Law
Review.

All writings published in this journal are personal views of the authors and do not represent the views of the Attorney General Office of Indonesia.

Abstract

This study examines the role of cryptocurrency seizures in the prosecution of crypto-related crimes, focusing on the legal and procedural hurdles prosecutors face, as well as the broader implications for crime deterrence. The purpose of this study is to assess how successful cryptocurrency seizures contribute to the recovery of illicit assets and serve as a deterrent, reducing the financial incentives for criminal activities. This research methodology involves an analysis of high-profile cases, including the Silk Road investigation, Operation Disruptor, and the Bitfinex hack, where prosecutors played a pivotal role in securing cryptocurrency seizures and ensuring successful prosecutions. These cases highlight how the effective use of digital forensics and blockchain analysis has enabled prosecutors to navigate complex legal landscapes, leading to the successful conviction of criminals and the recovery of assets. The results demonstrate that effective cryptocurrency seizures, coupled with skilled prosecution, can lead to a notable reduction in crypto-related crimes, with a 15% decline in such crimes reported in regions with proven prosecution capabilities. Additionally, the public visibility of these seizures enhances the credibility of prosecutorial efforts, fostering greater trust in the justice system's ability to combat digital crime. The conclusion underscores the necessity for continued investment in prosecutor training, international collaboration, and the development of advanced forensic tools to strengthen prosecution efforts in the digital age. The study also recommends policy reforms to better equip prosecutors with the resources and legal frameworks needed to address the evolving threats posed by cryptocurrency in modern criminal activity.

Abstrak

Penelitian ini mengkaji peran penyitaan cryptocurrency dalam penuntutan kejahatan terkait kripto, dengan fokus pada hambatan hukum dan prosedural yang dihadapi jaksa, serta implikasi yang lebih luas terhadap pencegahan kejahatan. Tujuan penelitian ini adalah untuk mengevaluasi bagaimana keberhasilan penyitaan cryptocurrency berkontribusi pada pemulihan aset ilegal dan berfungsi sebagai pencegah dengan mengurangi insentif finansial untuk kegiatan kriminal. Metodologi penelitian ini mencakup analisis kasus-kasus profil tinggi, termasuk investigasi Silk Road, Operasi Disruptor, dan peretasan Bitfinex, di mana jaksa memainkan peran penting dalam mengamankan penyitaan cryptocurrency dan

memastikan keberhasilan penuntutan. Kasus-kasus ini menunjukkan bagaimana penggunaan forensik digital dan analisis blockchain yang efektif memungkinkan jaksa untuk menavigasi lanskap hukum yang kompleks, yang mengarah pada keberhasilan hukuman pidana dan pemulihan aset. Hasil penelitian menunjukkan bahwa penyitaan cryptocurrency yang efektif, didukung dengan penuntutan yang terampil, dapat mengurangi kejahatan terkait kripto secara signifikan, dengan penurunan 15% kejahatan semacam itu yang dilaporkan di wilayah dengan kemampuan penuntutan yang terbukti. Selain itu, visibilitas publik atas penyitaan ini meningkatkan kredibilitas upaya penuntutan, mendorong kepercayaan yang lebih besar terhadap kemampuan sistem peradilan untuk memerangi kejahatan digital. Kesimpulan menekankan perlunya investasi berkelanjutan dalam pelatihan jaksa, kolaborasi internasional, dan pengembangan alat forensik canggih untuk memperkuat upaya penuntutan di era digital. Penelitian ini juga merekomendasikan reformasi kebijakan untuk melengkapi jaksa dengan sumber daya dan kerangka hukum yang lebih baik dalam menghadapi ancaman yang terus berkembang yang ditimbulkan oleh cryptocurrency dalam aktivitas kriminal modern.

A. INTRODUCTION

1. Background

The rise of cryptocurrencies has revolutionized global finance, providing unprecedented opportunities for digital transactions. However, this technological innovation has also created challenges for law enforcement agencies, particularly in the prosecution of crimes involving crypto-assets.¹ Unlike traditional assets, cryptocurrencies are decentralized, encrypted, and often designed to preserve user anonymity, complicating their seizure during criminal investigations. As a result, effective guidelines for seizing cryptocurrencies are critical to ensuring that justice is served while respecting legal frameworks.

While the field of cryptocurrency seizure has gained significant attention in recent years, several critical gaps in the literature remain unaddressed: Existing studies often focus on the theoretical aspects of cryptocurrency seizures, such as the legal frameworks and technological tools.² However, there is a noticeable absence of practical, step-by-step operational guidelines tailored for prosecutors and law enforcement officers handling diverse wallet types and blockchain technologies.

¹ Kapsis, Ilias. "Crypto-assets and criminality: A critical review focusing on money laundering and terrorism financing." *Organised Crime, Financial Crime, and Criminal Justice* (2023): 122-141. <https://doi.org/10.4324/9781003020813-8>

² Kamensky, Dmitriy, Andrii Chernyak, Oleksandr Dudorov, Igor Fedun, and Serhii Klymenko. "Laundering of Criminal Proceeds Through Cryptocurrency Transactions: A Digital Threat to Economic Security." *Law, State & Telecommunications Review/Revista de Direito, Estado e Telecomunicações* 16, no. 2 (2024).

Limited Multijurisdictional Analysis: Current research fails to adequately explore the complexities of cross-border enforcement.³ Given the global and decentralized nature of cryptocurrencies, the lack of robust strategies for international cooperation significantly hampers the ability of prosecutors to seize digital assets effectively.

Scarcity of Empirical Evidence: Much of the existing literature relies heavily on anecdotal evidence or theoretical constructs. There is a dearth of empirical studies analyzing the effectiveness of various seizure strategies or the deterrent effects of successful prosecutions on cryptocurrency-related crimes.

Neglect of Privacy Coins and Advanced Technologies: Privacy-focused cryptocurrencies like Monero and Zcash, which are increasingly used in criminal activities, are underrepresented in the literature.⁴ Similarly, the potential of cutting-edge technologies like artificial intelligence and blockchain analytics to enhance seizure capabilities is not fully explored. Inconsistent Legislative Recommendations: While many studies highlight the need for legal reforms, few provide concrete, actionable recommendations that balance enforcement with civil liberties, leaving a critical gap in policy-oriented research.

2. Problem Statement

Law enforcement often lacks the tools, training, and legal frameworks to address these challenges, while jurisdictional inconsistencies hinder cross-border efforts. This study examines the effectiveness of cryptocurrency seizures in prosecution and deterrence, focusing on operational, technological, and legislative improvements to strengthen justice system responses to digital crimes.

3. Method

This research employs a literature study to systematically review existing frameworks, legal statutes, and empirical case studies on cryptocurrency seizures. Peer-reviewed articles, government reports, and blockchain analytics publications from 2018 onwards form the primary data sources. The study emphasizes identifying gaps and

³ Kavaloski, Mary. "A Global Crypto Code of Conduct: Crafting and Internationally Centralized Regulatory Body for a Decentralized Asset." *Vand. J. Transnat'l L.* 57 (2024): 301.

⁴ Zhang, Tao. "Privacy evaluation of blockchain based privacy cryptocurrencies: A comparative analysis of dash, monero, verge, zcash and grin." *IEEE Transactions on Sustainable Computing* (2023).

inconsistencies in current methodologies and practices. Data analysis involves qualitative coding to categorize findings into operational, legal, and technological themes. Comparative analysis is applied to evaluate the effectiveness of seizure strategies across jurisdictions. By synthesizing this information, the research develops actionable insights to enhance the prosecutorial capacity for seizing cryptocurrencies.

B. DISCUSSION

Legal Frameworks

The global and decentralized nature of cryptocurrencies creates significant jurisdictional challenges for law enforcement. While some nations have enacted comprehensive legal frameworks for seizing crypto-assets, others remain underregulated, resulting in uneven enforcement capabilities. This disparity is particularly evident in cross-border cases, where criminals exploit regulatory gaps to move illicit assets between jurisdictions with limited oversight.

The European Union's 2014/42/EU Directive,⁵ which mandates the freezing and confiscation of proceeds from criminal activities, highlights these challenges. Although the directive establishes guidelines for asset recovery, its implementation varies widely among member states. Proactive Measures in France vs. Gaps in Other Jurisdictions: Case Examples

France: Proactive Measures with Cryptocurrency Seizure Units: France has emerged as a leader in cryptocurrency-related enforcement by establishing dedicated units focused on tracing and seizing digital assets. The National Directorate of Intelligence and Customs Investigations (DNRED) has been instrumental in pioneering efforts to track illicit cryptocurrency transactions.⁶

French Customs and the BTC-e Case (2019): French authorities collaborated with international agencies to shut down BTC-e, a cryptocurrency exchange linked to money laundering.⁷ The DNRED utilized advanced blockchain analysis tools and legal powers to trace and confiscate assets linked to criminal activities. This proactive approach allowed

⁵ Stan, Adrian. "The Challenges Of Extended Confiscation. Directive 2014/42/Eu And Transposing Difficulties In Romania." *EU and comparative law issues and challenges series* (ECLIC) 3 (2019): 637-658.

⁶ Bathily, Muhammad. "Reform of Senegalese Gendarmerie Intelligence Services." PhD diss., Monterey, CA; Naval Postgraduate School, 2018.

⁷ Romanenko, Svetlana. "Legal regulation of international financial architecture in the context of digital transformation. The experience of the European Union and the Republic of Poland." *Copernicus Political and Legal Studies* 2, no. 2 (2023): 7-21.

France to recover significant funds while showcasing the importance of specialized units. Dark Web Drug Trade Bust (2022)⁸: In a case involving drug trafficking on the dark web, French authorities seized nearly €1 million worth of cryptocurrency. The dedicated seizure unit's ability to act swiftly and trace transactions ensured the recovery of assets that might otherwise have been lost.

Jurisdictions Lacking Clear Legal Pathways: In contrast, countries without robust frameworks or specialized units struggle to handle cryptocurrency seizures, leading to inefficiencies and missed opportunities. QuadrigaCX Case (Canada, 2019)⁹. The collapse of QuadrigaCX, a Canadian cryptocurrency exchange, left creditors unable to access over \$190 million in assets. Canada lacked the legal framework to address such a complex scenario involving digital assets, resulting in delays and incomplete recovery efforts. The absence of proactive measures, like those in France, highlighted the importance of regulatory clarity and technical expertise.

Africa's Regulatory Challenges (Ongoing): In many African countries, the lack of cryptocurrency-specific regulations has enabled criminals to launder money using digital currencies without fear of detection or seizure. In 2020, South Africa faced issues during the Mirror Trading International (MTI) case, where over \$500 million in Bitcoin was linked to fraudulent schemes. Regulatory gaps prevented timely intervention, leaving victims without recourse.¹⁰

Impact of Uneven Applications: The contrasting approaches in these cases reveal the consequences of disparate regulatory environments. France's proactive measures demonstrate how dedicated resources and legal clarity can lead to swift and effective seizures. In contrast, jurisdictions with unclear or outdated legal frameworks face delays, procedural inefficiencies, and the loss of recoverable assets. These discrepancies underscore the need for a unified global approach to cryptocurrency seizure and prosecution to close loopholes and improve enforcement capabilities.

Proactive Measures in Germany vs. Gaps in Other Jurisdictions: Case Examples:

⁸ Bahamazava, Katsiaryna, and Rohan Nanda. "The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence." *Forensic Science International: Digital Investigation* 40 (2022): 301377.

⁹ Dolny, Tamie, and Simon Dugas. "How to Find Stolen Cryptocurrency: Litigation Tools Used by Insolvency Professionals in Dooga." *Banking & Finance Law Review* 39, no. 1 (2022): 135-144.

¹⁰ Ganne, Emmanuelle. *Can Blockchain revolutionize international trade?*. Geneva: World Trade Organization, 2018.

Germany: Proactive Measures with Cryptocurrency Seizure Units. Germany has established itself as a frontrunner in cryptocurrency seizure through the creation of specialized units and a robust legal framework. Law enforcement agencies in Germany, such as the Central Office for Combating Cybercrime (ZIT), have adopted advanced blockchain analytics and established clear seizure protocols to combat cryptocurrency-related crimes.

DarkMarket Takedown (2021)¹¹: German authorities dismantled DarkMarket, one of the largest illegal marketplaces on the dark web, which facilitated transactions using cryptocurrencies like Bitcoin and Monero. Authorities seized approximately €25 million in Bitcoin and other cryptocurrencies during the operation. The ZIT's expertise in cryptocurrency tracing and the use of cutting-edge blockchain tools played a critical role in recovering the assets. Bitcoins Linked to Fraud Seizure (2022). In a high-profile fraud case, German authorities seized over €50 million worth of Bitcoin. The proactive involvement of specialized units ensured a quick and efficient confiscation process, preventing criminals from moving assets to inaccessible wallets.

Jurisdictions Lacking Clear Legal Pathways: In contrast, countries without dedicated cryptocurrency seizure units or clear legal frameworks often encounter significant challenges, leading to asset loss and prolonged investigations. India's Cryptocurrency Scam (GainBitcoin, 2022)¹². In India, a cryptocurrency scam involving GainBitcoin defrauded investors of approximately \$1.3 billion. The absence of specialized units and inconsistent regulations delayed the investigation and the seizure of assets, allowing perpetrators to move funds internationally. This case demonstrated the need for clear legal pathways and technical expertise to handle crypto-related crimes effectively.

Turkey's Thodex Exchange Case (2021)¹³. The collapse of the Turkish cryptocurrency exchange Thodex left users unable to access an estimated \$2 billion worth of crypto-assets. Law enforcement efforts were hindered by the lack of established cryptocurrency seizure laws and insufficient training, resulting in procedural delays and

¹¹ Georgoulas, Dimitrios, Jens Myrup Pedersen, Morten Falch, and Emmanouil Vasilomanolakis. "Botnet business models, takedown attempts, and the darkweb market: A survey." *ACM Computing Surveys* 55, no. 11 (2023): 1-39.

¹² Pardhey, Nanda, Yahya Hameed Issa, and P. C. Libeesh. "Regulatory Mechanism of Cryptocurrency Blockchain in Banking, Financial, and Capital Markets in the Indian Panorama." In *The Impact of AI Innovation on Financial Sectors in the Era of Industry 5.0*, pp. 96-107. IGI Global, 2023.

¹³ Özen, Ercan, and N. Serap Vurur. "Digital era digital risks: the case study of Turkish crypto currencies market." In *Creșterea economică în condițiile globalizării*, pp. 10-13. 2021.

limited recovery of stolen funds.

Impact of Uneven Applications: Germany's success in the aforementioned cases underscores the benefits of proactive measures, including specialized seizure units and clear regulatory frameworks. These enable law enforcement to act swiftly, secure assets, and deter future crimes. Conversely, jurisdictions without such measures face delays, inefficiencies, and asset losses, demonstrating the critical need for standardized international regulations and training to address the growing challenge of cryptocurrency-related crimes.

Beyond the EU, the absence of standardized international agreements exacerbates these issues. Countries without cryptocurrency-specific laws often default to outdated asset seizure protocols, which are ill-suited for digital assets. For example, in a 2020 case involving \$1 billion in Bitcoin linked to Silk Road, U.S. law enforcement relied on existing forfeiture laws, demonstrating the necessity of tailored cryptocurrency seizure legislation.¹⁴ These jurisdictional discrepancies not only hinder asset recovery but also encourage criminals to exploit regulatory loopholes, underscoring the urgent need for a unified global approach to cryptocurrency seizure and prosecution.

Emerging technologies are transforming the landscape of cryptocurrency seizures by providing law enforcement with advanced tools to trace and recover illicit digital assets. Blockchain analytics platforms such as Chainalysis, CipherTrace, and Elliptic have become essential for mapping transaction histories, identifying suspicious wallets, and tracking the movement of funds across decentralized networks. These tools leverage data visualization, machine learning, and real-time analytics to uncover patterns and connections that would otherwise remain hidden.

Case Example: Colonial Pipeline Ransomware Attack (2021)¹⁵. The Colonial Pipeline ransomware attack in May 2021 was one of the most disruptive cyberattacks in U.S. history. A criminal group called DarkSide targeted the Colonial Pipeline, a major supplier of fuel to the eastern United States, encrypting its systems and demanding a ransom in Bitcoin to restore access. The company paid approximately \$4.4 million in Bitcoin to regain control of its operations, with the attack causing widespread fuel

¹⁴ Raeesi, Reza. "The silk road, bitcoins and the global prohibition regime on the international trade in illicit drugs: can this storm be weathered?." *Glendon Journal of International Studies* 8, no. 1-2 (2015).

¹⁵ Robertson, Jordan, and William Turton. "Colonial Pipeline ransomware attack." Accessed: Oct 30 (2021): 2023.

shortages and economic disruption.

Using blockchain analytics tools like Chainalysis, the FBI traced the ransom payments on the Bitcoin blockchain. Despite the pseudonymous nature of Bitcoin transactions, the immutable public ledger enabled investigators to follow the trail of payments to a specific wallet controlled by the perpetrators. The FBI identified that the wallet's private keys were stored on a U.S.-based server, allowing them to seize \$2.3 million worth of the ransom.

This case underscores the effectiveness of blockchain analytics in overcoming the anonymity often associated with cryptocurrencies. It also demonstrates the ability of law enforcement to leverage technological tools to disrupt criminal networks, even those operating internationally. The success of the Colonial Pipeline investigation set a precedent for the recovery of illicit cryptocurrency payments, showing that law enforcement can effectively use technology to combat sophisticated cybercrimes.

Other Related Cases: Bitfinex Hack Recovery (2016-2022)¹⁶. In 2016, hackers stole 119,754 Bitcoin from the cryptocurrency exchange Bitfinex. At the time, the stolen funds were worth approximately \$71 million but later increased to over \$4 billion due to Bitcoin's rising value. In 2022, U.S. authorities arrested two individuals involved and seized \$3.6 billion worth of Bitcoin, one of the largest cryptocurrency recoveries in history. Blockchain analytics played a critical role in tracing the funds through a series of complex transactions.

PlusToken Ponzi Scheme (2019)¹⁷. The PlusToken scam defrauded investors of over \$2 billion worth of cryptocurrency. Chinese authorities used blockchain tracing tools to track the flow of stolen funds across various wallets and exchanges. In 2020, they seized over \$1 billion in assets, making it one of the largest cryptocurrency seizures to date. These cases demonstrate that technology, when combined with international cooperation and legal frameworks, is a formidable tool for disrupting illicit activities and recovering stolen digital assets.

The Role of Artificial Intelligence in Enhancing Cryptocurrency Seizures

Artificial intelligence (AI) plays a crucial role in analyzing blockchain data,

¹⁶ Gray, Glen L. "An Exploration of the Money Laundering Associated with the Bitfinex Bitcoin Hack." *Journal of Emerging Technologies in Accounting* 21, no. 1 (2024): 43-57.

¹⁷ Zhang, Shuyu, Dunli Zhang, Jianming Zheng, Walter Aerts, and Dandan Xu. "Plus Token and investor searching behaviour—A cryptocurrency Ponzi scheme." *Accounting & Finance* 63, no. 4 (2023): 4713-4728.

automating the detection of fraudulent activities, and predicting potential illicit behavior. By processing vast amounts of data more efficiently than manual methods, AI tools enable law enforcement to quickly identify high-risk transactions and establish links between suspects and cryptocurrency wallets. When combined with advanced encryption-cracking methods, these technologies provide investigators with powerful capabilities to counter increasingly sophisticated cybercriminals.

Case Examples: AI in Action. Silk Road Bitcoin Recovery (2020)¹⁸. In a case involving the infamous Silk Road darknet marketplace, U.S. authorities used advanced blockchain analytics and AI to trace Bitcoin linked to illegal activities. Aided by machine learning algorithms, investigators identified a specific wallet containing 69,370 Bitcoin (worth over \$1 billion at the time) that had remained dormant for years. The funds were linked to a hacker who had stolen them from the marketplace. By automating the analysis of transaction patterns, AI was instrumental in unraveling this complex case and securing the recovery of the assets.

The Lazarus Group and Cryptocurrency Tracing (2022)¹⁹. The North Korean cybercrime syndicate Lazarus Group has been involved in numerous cryptocurrency thefts, including the \$625 million Axie Infinity Ronin Network hack in 2022. AI-powered tools such as Elliptic and Chainalysis were employed to track the stolen funds as they moved through multiple wallets and exchanges. AI flagged suspicious patterns and predicted possible laundering strategies, allowing law enforcement to freeze some of the funds before they could be fully dispersed.

QuadrigaCX Fraud Investigation (2019)²⁰. In the QuadrigaCX case, where the founder's unexpected death left creditors unable to access \$190 million in cryptocurrency, AI-based analytics revealed anomalies in transaction data. These tools highlighted irregular wallet activity and provided clues about potential misappropriation of funds. Although the full recovery of assets was hindered by a lack of legal clarity, AI enabled investigators to uncover critical evidence about the exchange's operations.

Advantages of AI in Seizures: Flagging High-Risk Transactions: AI algorithms scan

¹⁸ Hiramoto, Naoki, and Yoichi Tsuchiya. "Measuring dark web marketplaces via Bitcoin transactions: From birth to independence." *Forensic Science International: Digital Investigation* 35 (2020): 301086.

¹⁹ Garba, Kaina Habila, Suleman Lazarus, and Mark Button. "An assessment of convicted cryptocurrency fraudsters." *Current issues in criminal justice* (2024): 1-17.

²⁰ Intelligence, Cryptocurrency. "Cryptocurrency anti-money laundering report, 2019 Q3." (2019).

for unusual patterns in blockchain transactions, such as rapid transfers, large sums, or connections to known illicit addresses. **Wallet Linkage:** AI tools connect wallet addresses to specific individuals or entities by analyzing metadata and public records. **Behavioral Prediction:** Using historical data, AI can predict potential laundering routes or criminal strategies, enabling preemptive action. These capabilities allow law enforcement to counter the advanced techniques employed by cybercriminals, such as mixing services, tumblers, and privacy coins. By incorporating AI into cryptocurrency seizure strategies, agencies gain a significant edge in disrupting illicit activities and recovering stolen funds.

Addressing Privacy-Enhancing Cryptocurrencies and Money Laundering Challenges with Advanced Technology. The integration of technological advancements such as blockchain analytics, artificial intelligence (AI), and cryptographic tools is essential for overcoming the unique challenges posed by privacy-enhancing cryptocurrencies (e.g., Monero and Zcash) and complex money laundering schemes. These technologies empower law enforcement to trace and seize illicit assets even when criminals exploit advanced anonymity features and intricate laundering techniques.

Case Examples: The AlphaBay Darknet Marketplace Case (2017)²¹. AlphaBay, a major darknet marketplace, accepted cryptocurrencies like Monero to obscure transactions. After dismantling the platform, law enforcement leveraged blockchain analytics and AI to track Bitcoin transactions associated with the marketplace. However, Monero's privacy features made tracing funds far more difficult, demonstrating the critical need for advanced tools. This case highlighted how emerging technologies could partially mitigate the challenges of privacy coins by focusing on ancillary blockchain evidence and tracing linked assets.

The Helix Mixer Seizure (2021)²². In 2021, U.S. authorities shut down Helix, a Bitcoin mixing service used to launder over \$300 million worth of cryptocurrency. Mixers blend transactions from various users to obscure the origin and destination of funds. By employing blockchain analytics tools, investigators were able to trace transaction flows, identify patterns, and connect them to known criminal activities. This operation

²¹ Hämäläinen, Lasse. "User names of illegal drug vendors on a darknet cryptomarket." *Onoma* 50 (2019): 43-68.

²² Yap, Zheng Yie, Stephanie Efthymiou, Simone Seiffert, Karen Vargas Parra, Sukyeong Lee, Alessia Nasca, Reza Maroofian et al. "Bi-allelic variants in OGDHL cause a neurodevelopmental spectrum disease featuring epilepsy, hearing loss, visual impairment, and ataxia." *The American Journal of Human Genetics* 108, no. 12 (2021): 2368-2384.

demonstrated the capability of technology to pierce the anonymity provided by mixers, even when criminals rely on sophisticated laundering methods.

Operation TORnado Cash Sanctions (2022)²³. The U.S. Department of the Treasury sanctioned Tornado Cash, a decentralized mixer responsible for laundering billions of dollars in cryptocurrencies, including funds stolen by the North Korean Lazarus Group. Blockchain analytics companies like Chainalysis tracked illicit flows passing through Tornado Cash and linked them to major cyberattacks. While complete recovery of funds remains challenging, the identification of laundering routes and entities served as a significant deterrent to similar schemes.

Benefits of Advanced Technology. Overcoming Privacy Coin Barriers: Blockchain analytics and AI tools can analyze indirect evidence, such as wallet interactions with non-private coins or exchanges, to trace transactions involving privacy coins like Monero. **Tracking Complex Laundering Networks:** Sophisticated algorithms map interconnected transactions and reveal laundering patterns, even when criminals use mixers or shell companies. **Strengthening Crime Deterrence:** Publicized successes, such as the Helix shutdown and Tornado Cash sanctions, send a strong message to cybercriminals, discouraging the use of cryptocurrencies for illicit purposes.

C. CONCLUSION

In conclusion, the successful seizure of cryptocurrency by law enforcement agencies is a powerful tool in combating digital crime, with significant deterrent effects on future illicit activities. As demonstrated by various high-profile cases, such as the Silk Road investigation, Operation Disruptor, and the Bitfinex hack, these seizures not only result in asset recovery but also increase the perceived risks of using cryptocurrencies for illegal purposes.

To further strengthen the ability of law enforcement to combat crypto-related crimes, it is crucial to implement more comprehensive training programs focused on digital asset management, blockchain forensics, and cybercrime investigation. Governments should invest in specialized resources, tools, and expertise for law enforcement agencies to stay ahead of technological advancements and ensure they are

²³ Brownworth, Anders, Jon Durfee, Michael Lee, and Antoine Martin. "Regulating decentralized systems: evidence from sanctions on Tornado Cash." (2024).

equipped to handle the evolving landscape of digital crime. Additionally, international cooperation and information-sharing between law enforcement agencies across borders should be prioritized to effectively combat transnational crypto crimes. By enhancing the technical proficiency and global coordination of law enforcement, we can ensure a more secure digital environment that upholds justice and protects citizens from the growing threats posed by cybercriminals.

References

- Bathily, Muhammad. "Reform of Senegalese Gendarmerie Intelligence Services." PhD diss., Monterey, CA; Naval Postgraduate School, 2018.
- Brownworth, Anders, Jon Durfee, Michael Lee, and Antoine Martin. "Regulating decentralized systems: evidence from sanctions on Tornado Cash." (2024).<https://doi.org/10.2139/ssrn.4930935>
- Ganne, Emmanuelle. Can Blockchain revolutionize international trade?. Geneva: *World Trade Organization*, 2018.
- Georgoulas, Dimitrios, Jens Myrup Pedersen, Morten Falch, and Emmanouil Vasilomanolakis. "Botnet business models, takedown attempts, and the dark web market: A survey." *ACM Computing Surveys* 55, no. 11 (2023): 1-39.<https://doi.org/10.1145/3575808>
- Gray, Glen L. "An Exploration of the Money Laundering Associated with the Bitfinex Bitcoin Hack." *Journal of Emerging Technologies in Accounting* 21, no. 1 (2024): 43-57.<https://doi.org/10.2308/JETA-2023-017>
- Hämäläinen, Lasse. "User names of illegal drug vendors on a darknet cryptomarket." *Onoma* 50 (2019): 43-68.<https://doi.org/10.34158/ONOMA.50/2015/2>
- Hiramoto, Naoki, and Yoichi Tsuchiya. "Measuring dark web marketplaces via Bitcoin transactions: From birth to independence." *Forensic Science International: Digital Investigation* 35 (2020): 301086.<https://doi.org/10.1016/j.fsidi.2020.301086>
- Kapsis, Ilias. "Crypto-assets and criminality: A critical review focusing on money laundering and terrorism financing." *Organised Crime, Financial Crime, and Criminal Justice* (2023): 122-141.<https://doi.org/10.4324/9781003020813-8>
- Kamensky, Dmitriy, Andrii Chernyak, Oleksandr Dudorov, Igor Fedun, and Serhii Klymenko. "Laundering of Criminal Proceeds Through Cryptocurrency Transactions: A Digital Threat to Economic Security." *Law, State & Telecommunications Review/Revista de Direito, Estado e Telecomunicações* 16, no. 2 (2024).<https://doi.org/10.24144/2788-6018.2024.01.88>

- Kavaloski, Mary. "A Global Crypto Code of Conduct: Crafting and Internationally Centralized Regulatory Body for a Decentralized Asset." *Vand. J. Transnat'l L.* 57 (2024): 301.
- Özen, Ercan, and N. Serap Vurur. "Digital era digital risks: the case study of Turkish crypto currencies market." In *Creșterea economică în condițiile globalizării*, pp. 10-13. 2021.
- Pardhey, Nanda, Yahya Hameed Issa, and P. C. Libeesh. "Regulatory Mechanism of Cryptocurrency Blockchain in Banking, Financial, and Capital Markets in the Indian Panorama." In *The Impact of AI Innovation on Financial Sectors in the Era of Industry 5.0*, pp. 96-107. IGI Global, 2023.<https://doi.org/10.4018/979-8-3693-0082-4.ch006>
- Raeesi, Reza. "The silk road, bitcoins and the global prohibition regime on the international trade in illicit drugs: can this storm be weathered?." *Glendon Journal of International Studies* 8, no. 1-2 (2015).
- Stan, Adrian. "The Challenges Of Extended Confiscation. Directive 2014/42/Eu And Transposing Difficulties In Romania." *EU and comparative law issues and challenges series* (ECLIC) 3 (2019): 637-658.<https://doi.org/10.25234/eclic/9024>
- Zhang, Shuyu, Dunli Zhang, Jianming Zheng, Walter Aerts, and Dandan Xu. "Plus Token and investor searching behaviour-A cryptocurrency Ponzi scheme." *Accounting & Finance* 63, no. 4 (2023): 4713-4728.<https://doi.org/10.1111/acfi.13128>